AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: s/Tiffany Noble

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF:)
SEVENTEEN WIRELESS CELL PHONES)
CURRENTLY STORED IN THE CUSTODY OF USPIS)
LOCATED AT 6500 AIR CARGO RD)
OKLAHOMA CITY, OK 73195)

Case No: M-22-575-SM

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following Property:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violations of:

Code Sections	*Offense Descriptions*
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1708	Mail Theft
18 U.S.C. § 1349	Conspiracy to Commit Mail or Wire Fraud

The application is based on these facts:

See attached Affidavit of Special Agent Chris Nicholson, United States Postal Inspector Service, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____days is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Chris Nicholson
Special Agent, United States Postal Inspector Service

Sworn to before me and signed in my presence.

Date: Aug. 11, 2022

Judge's signature

City and State: Oklahoma City, Oklahoma

Suzanne Mitchell, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF: SEVENTEEN WIRELESS CELL PHONES CURRENTLY STORED IN THE CUSTODY OF USPIS LOCATED AT 6500 AIR CARGO RD OKLAHOMA CITY, OK 73195	)	**M-22-** 575-SM

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Chris Nicholson, being duly sworn, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property— seventeen wireless cell phones of various make, model, and color, as described in Attachment A, that are currently stored in the custody of the United States Postal Inspection Service (USPIS) located at 6500 Air Cargo Road, Oklahoma City, Oklahoma 73195—and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Postal Inspector with USPIS and have been so employed since December 2021. I am currently assigned to the USPIS Fort Worth Division domiciled in Oklahoma City, Oklahoma. I am responsible for conducting investigations of crimes

against the United States Postal Service in violation of federal law(s). My duties include the investigation of illegal mailings and Mail Fraud which violates Title 18, United States Code, Section 1341 (mail theft).

3. Prior to working as an Inspector for USPIS, I gained investigative experience as a Special Agent with the Naval Criminal Investigative Service (NCIS) from September 2017 to December 2021. My NCIS duties included, but were not limited to, investigating crimes committed against United States Navy assets and personnel worldwide, including allegations of espionage, fraud, theft, sexual assault, aggravated assault, child exploitation, and illegal drugs. My investigative experience has also been supplemented with numerous hours of participation with local and state law enforcement task forces to stay apprised of evolving criminal methodology.

4. Prior to my work with NCIS, I was employed by the Dallas Police Department (DPD) from March 2007 to July 2013 as a Police Officer certified by the Texas Commission on Law Enforcement Standards and Education Basic Training Academy. During my time with DPD, I held investigative positions within burglary, narcotics, organized crime, and fugitive recovery squads. My employment with DPD required yearly in-service training, which included refresher courses in surveillance, warrant execution, tactics, criminal intelligence, and interview techniques. From 2013 to 2017, I was also employed as a Police Officer with the City of Kenner, Louisiana where I continued to perform the aforementioned duties.

5. Since becoming a Federal Agent, I have competed the Criminal Investigator Training Program and NCIS Special Agent Basic Training Academy at the

Federal Law Enforcement Training Center (FLETC), in Brunswick, Georgia, which included instruction in the investigation of federal, state, and local crimes.

6. While employed in a law enforcement capacity, I have made arrests for the aforementioned criminal activities and participated in the execution of approximately 100 search and seizure warrants authorized by federal and state judges. Throughout the last 15 years of my law enforcement career, I have conducted and assisted in numerous activities, to include, but not limited to, investigations, interviews, arrests, and the execution of search and seizure warrants, for crimes to include fraud.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. The property to be searched includes seventeen wireless cell phones of various make, model, and color (herein referred to as the "**TARGET DEVICES**") as further described in **Attachment A** (physical description), for evidence of violations of federal law, to wit: 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1708 (mail theft); 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); and 18 U.S.C. § 1349 (conspiracy to commit mail or wire fraud), as described further in **Attachment B** (description of items to be seized). The **TARGET DEVICES** are:

i. Black Apple iPhone model# A1660 SIM# 8901260055977818269 07.00 PEAP# IS0001505865;

ii. Gold Samsung Galaxy S7 IMEI# 359775071814012 2 PEAP# IS0001505866;

iii. Silver Apple iPhone model# A1688 PEAP# IS0001505867;

iv. Black Apple iPhone SIM# 89012600739246705 50M21.02 PEAP# IS0001505868;

v. Black Apple iPhone SIM# SM128PSIMT5TOD8901260955188263736 PEAP# IS0001505869;

vi. Blue Samsung Galaxy S6 IMEI# 99000704798119316.07 PEAP# IS0001505870;

vii. Gold Apple iPhone SIM# 89014104274488AO40262888773335 PEAP# IS0001505871;

viii. Black Samsung Galaxy S7 PEAP# IS0001505872;

ix. Blue Samsung Galaxy S6 IMEI# 9900070494339516.11 PEAP# IS0001505873;

x. Black Apple iPhone PEAP# IS0001505874;

xi. Blue Apple iPhone SIM# 89148000006497258234 PEAP# IS0001505875;

xii. Red Apple iPhone SIM# 89012602417333399031086 48 PEAP# IS0001505876;

xiii. Black Samsung Galaxy S7 IMEI# 359764081434928 PEAP# IS0001505877;

xiv. Silver Samsung Galaxy S8 IMEI# 357723081373066 PEAP# IS0001505878;

xv. Silver Samsung Galaxy S7 IMEI# 358166075659265 PEAP# IS0001505879;

xvi. Silver Apple iPhone model# A1586 IMEI# 359263067022856 PEAP# IS0001505880;

xvii. Gold Apple iPhone model# A1586 IMEI# 356977062704829 PEAP# IS0001505881.

Some of the **TARGET DEVICES** are locked or damaged preventing investigators from obtaining additional specific identifying phone information such as a model or serial number. The **TARGET DEVICES** are currently stored in the custody of the USPIS at 6500 Air Cargo Road, Oklahoma City, Oklahoma 73195 (Western District of Oklahoma).

8. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

9. This Affidavit is based upon my personal investigation and information received by me from other law enforcement officers and agents. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

10. On June 1, 2021, Oklahoma County Sheriff's Office (OCSO) deputies were patrolling the area of I-35 and NE 122nd Street in Oklahoma City, Oklahoma, when they observed several traffic violations (not signaling 100 feet before changing lanes with other traffic present and dark tinted windows) performed by a Blue Chevrolet Malibu equipped with Florida license plate EVVB66. Upon contacting the vehicle, deputies observed five occupants who were subsequently identified as Jason Fredy Darbouze, Nathan Tyrell Omega, Donald Preston Brown III, Evans Soiuilien, and Dimitris Shamar Simon. Deputies also detected the strong odor of marijuana. A probable cause search of the vehicle was conducted revealing approximately 18 grams of marijuana, 17 cell phones, and 158 gift cards (Target and Walgreens), which were a mix of loose and new-in-packaging cards. OCSO also related one of the occupants dropped something behind the vehicle seat, which was recovered and found to be mail displaying Oklahoma unemployment insurance information mailed to an Oklahoma address and a name not matching any of the vehicle occupants.

11. Deputies also located four miscellaneous cards within the vehicle with different people's names including a Florida ID card belonging to a Brian McKnight. Additional items located inside the vehicle by OCSO were described as pieces of mail

containing pre-paid Mastercard information from an Oklahoma resident who was not an occupant of the vehicle

12. Using the identification numbers from the recovered Target gift cards, OCSO obtained transaction data from Target which included the date and time the gift cards were purchased from Target registers. OCSO was then able to locate Target asset protection images and video footage, dated June 1, 2021, showing two black males purchase gift cards at Target self-checkout registers by scanning different cell phones to perform payment. The video also showed a third black male attempt to make a purchase but left his items at the register and walked away. Prior to the entering Target, video footage shows the same three black males gathering in the Target parking lot by a Blue Chevrolet Malibu equipped with a Florida license plate ending in 66, one of which can be seen opening the driver's door to the vehicle. Additional information obtained from Target revealed a cellular phone application, instead of cash or debit card, was used to purchase these cards which totaled an approximate value of $5,575.00.

13. Due to suspected identity theft, mail theft, mail fraud, wire fraud, and conspiracy, this investigation was adopted by USPIS in December 2021.

14. USPIS subsequently obtained business records from Target regarding the gift cards recovered by OCSO deputies in the traffic stop on June 1, 2021. According to Target's records, the gift cards were purchased at cash registers using cell phones containing an Apple Pay account.

15. USPIS obtained additional purchase records from Target which revealed the Apple Pay account (ending in 5419) was funded by a Visa Gold Credit card issued in

the Country of Romania. USPIS contacted representatives of Visa who advised the 16-digit number associated with the card did not exist within their banking system.

16. USPIS also obtained Walgreens business records related to the Walgreens gift cards recovered by OCSO deputies in the traffic stop on June 1, 2021. According to Walgreens' records, the gift cards were purchased using a Walgreens rewards cellular phone application under names that did not match any of the occupants detained by OCSO. Further investigative inquiries revealed one Walgreens rewards account was under the name of an individual who died in 2015. A second Walgreens rewards account was listed in the name of an individual who died in 2020.

17. USPIS also conducted a vehicle history inquiry on the Blue Chevrolet Malibu using the equipped Florida license plate EVVB66. Results indicated the vehicle was a rental owned by Enterprise Rent-a-Car. Additional records obtained from Enterprise revealed the Malibu was rented by Donald Preston Brown on May 4, 2021, in Hialeah, Florida before being driven to Oklahoma City, Ok.

BACKGROUND ON UNEMPLOYMENT INSURANCE PROGRAMS

18. The Unemployment Insurance Program ("UI Program") is a joint federal-state partnership administered on behalf of the U.S. Department of Labor by state workforce agencies ("SWA"), also known as UI agencies. The UI program is designed to provide benefits to persons who are out of work through no fault of their own. Each state administers a separate UI Program within guidelines established under federal law. UI Program benefits are generally funded through employment taxes paid by employers and collected by the state. These revenues are deposited into the federal Unemployment Trust

Fund (UTF), which is held by the United States Treasury. Each state holds an account within the UTF. *See* 18 U.S.C. § 1104(a) ("There is hereby established in the Treasury of the United States a trust fund to be known as the 'Unemployment Trust Fund' . . . The Secretary of the Treasury is authorized and directed to received and hold in the Fund all moneys deposited therein by a State agency from a State unemployment fund.").

19. The Oklahoma Employment Security Commission (OESC) is the state workforce agency tasked with administering the UI Program in Oklahoma.

20. In order to qualify for traditional UI benefits, the applicant must have earned wages which were taxed for a qualifying period of time. Self-employed individuals, independent contractors, and non-traditional workers, whose income is outside of a traditional employment relationship and not subject to employment taxes, are generally not covered by UI programs.

21. On March 27, 2020, the CARES Act provided additional federal assistance to workers who would otherwise not qualify for traditional UI benefits. The CARES Act provided assistance in the form of Pandemic Unemployment Assistance ("PUA"), Pandemic Emergency Unemployment Compensation ("PEUC") and Federal Pandemic Unemployment Compensation ("FPUC").

22. PUA generally provides benefits to certain individuals who would not qualify for traditional UI programs, and are unemployed, partially unemployed, or unable to work due to COVID-19 related reasons. Individuals who are able to telework with pay are not eligible for PUA assistance. PUA initially provided up to 39 weeks of benefits to qualifying individuals which were set to expire on December 31, 2020. On or about

December 27, 2020, the Continued Assistance for Unemployed Workers of 2020 Act was signed into law. This Act extended the payment of PUA benefits for up to 50 weeks through March 14, 2021. Then on March 11, 2021, the American Rescue Plan Act of 2021 ("ARPA") was signed into law. Under ARPA, PUA benefits for up to 79 weeks have been extended through September 6, 2021. The PUA program is administered by the SWA/UI agency in each state, but the benefits are 100% funded by the federal government. A PUA claim is a claim for benefits against income earned or expected to be earned by the claimant in a particular state. The claimant must certify to the particular SWA/UI agency administering the benefits that the claimant is able to go to work each day, and, if offered a job, the claimant must be able to accept it. The claimant must certify this information on a weekly basis during the benefits period. The claimant is also responsible for reporting any income earned on a weekly basis to the SWA/UI agency to which they submitted a claim.

23. PEUC was established to extend the term for UI benefits and provided up to an additional 13 weeks of UI benefits to individuals who have exhausted their regular UI benefits under state or federal law and have no rights to UI under any other federal state or law. Under the Continued Assistance for Unemployed Workers of 2020 Act, PEUC benefits were extended to provide an additional 11 weeks of benefits for a maximum of 24 weeks through March 14, 2021. Under ARPA, PEUC benefits have been extended for up to 53 weeks through September 6, 2021.

24. Separately, FPUC provided an additional $600 per week in benefits through July 2020, to individuals who were collecting UI, PUA and PEUC benefits.

25. FPUC benefits are 100% funded by the federal government. From August 1, 2020, through September 5, 2020, PUA and UI claimants were eligible to receive Federal Lost Wage Assistance ("FLWA") in the amount of $300 per week funded by the Federal Emergency Management Agency ("FEMA"). Under the Continued Assistance for Unemployed Workers of 2020 Act, an additional $300 in weekly FPUC benefits was extended from December 26, 2020 through March 14, 2021. Then under ARPA, FPUC benefits of $300 have been extended through September 6, 2021.

26. Since about April 2020, DOL-OIG, along with other law enforcement agencies, has been investigating an influx of fraudulent UI claims submitted to state UI programs, including OESC, during the COVID-19 pandemic. The influx of fraudulent UI claims is, at least in part, attributable to the additional federal dollars that have been pumped into state UI programs to assist workers during the pandemic.

27. In Oklahoma, to receive weekly UI Program benefits, claimants must certify that they are able, available and actively seeking full-time employment. Claimants may file for weekly benefits in one of the two ways: (1) the telephone; (2) an online application system.

28. To receive UI Program benefits, a claimant is required to provide information to OESC, via the telephone or internet, including their name, mailing address, social security number (SSN), date of birth, last employer and separating employer's name and address and reason for separation. If the claimant files for UI Program benefits via the internet, they are required to enter their name, e-mail address, and establish security questions. Along with entering the SSN and answering the

questions, they will establish a claim ID number and a four-digit PIN with OESC. The claimant establishes their own four-digit PIN, but the system establishes the claim ID number. The claim ID number and a four-digit PIN can then be used in future log-ins to access claim information online.

29. After a claimant has applied for and has been determined monetarily eligible for benefits, a weekly request for benefits (sometimes referred to as a "weekly certification") must be filed for each week they are requesting benefits. Claimants must submit a timely request for weekly benefits/weekly certification. The weekly request for benefits/weekly certifications can be filed through the OESC online system.

30. OESC contracts with Conduent, a third-party financial services provider, to process UI benefit payments. Each night, OESC submits batch files containing claimant information (claimants' name, date of birth, address, phone number and SSN) to Conduent to establish UI Program debit card accounts for claimants. OESC, through its partner relationships, transfers funds to Conduent to fund the debit cards. Conduent produces and mails a debit card from its facility in Austin, Texas to the claimant's address reflected in the OESC database. New and replacement cards are sent via the U.S. mail to the claimant's address and may be sent via FedEx or UPS if an expedite is specifically requested. The UI Program debit card account is established only for the purpose of paying UI Program benefits. The claimant can withdraw the money transferred to the debit card account at will for any purpose, including for cash.

BACKGROUND REGARDING CELLULAR DEVICES

31. Based upon my training and experience, I am aware that individuals involved in fraudulent activity often use cellular phones to maintain contact with co-conspirators and purchasers of information illegally obtained from the U.S. Mail system. Such cell phones and their associated memory cards commonly contain electronically stored information which constitutes evidence, fruits, and instrumentalities of fraud offenses including, but not limited to, the phone directory and/or contacts list, calendar, text messages, voicemail, e-mail messages, call logs, photographs, , and videos. Additional items commonly found on cell phones are applications or "apps" that are self-contained programs designed to enhance functionality. Some of these apps include those such as Apple Wallet or Walgreens which are used to purchase items in lieu of cash or a debit card. Both Apple Wallet and the Walgreens app require an account, created by the user, which includes personal and financial information. Once the account is completed, the app, combined with the cell phone, can be used for a convenient transaction experience.

32. Based upon my training and experience, I am aware that individuals involved in fraudulent activity often drop or switch phones to avoid detection by law enforcement, and often have multiple phones that they use for different co-conspirators in order to distance themselves from criminal activity. I am further aware that individuals involved in fraudulent activity often keep old cellular telephones no longer in use to save telephone numbers of co-conspirators, as well as other relevant information including text messages and photographs.

33. Based upon my training and experience, I am aware that individuals involved in fraudulent activity oftentimes have stored videos and/or text and voice messages maintained on their cell phones, which are associated with the use of fraudulently obtained mail and the proceeds derived from its use for furthering criminal activity.

34. Based upon my training and experience, I am aware that individuals involved in fraudulent activity often use coded words and phrases, as well as extremely vague conversations, in order to discuss their plans and prevent anyone from overhearing or recognizing that the subject matter involves illegal activity.

35. Based upon my training and experience, I am aware that individuals involved in fraudulent activity often use cellular telephones to perform payments for various items via the use of commercial financial applications such as Apple Wallet, Apple Pay, Google Pay, Cash App, and Venmo. These financial applications require stored credit cards and/or bank account numbers, which, when involved in fraud, are commonly created from information illegally obtained from the US Mail system.

TECHNICAL TERMS

36. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with

other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

37. Based on my knowledge, training, and experience I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **TARGET DEVICES** were used, the purpose of such use, who used the devices, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data

stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

40. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

41. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET DEVICES** described in Attachment A to seek the items described in Attachment B.

CHRIS NICHOLSON
United States Postal Inspector
United States Postal Inspection Service

Sworn and subscribed to before me this 11th day of August 2022.

SUZANNE MITCHELL
United States Magistrate Judge
Western District of Oklahoma

ATTACHMENT A

The property to be searched includes seventeen wireless cell phones of various make, model, and color (herein referred to as the "**TARGET DEVICES**"), including:

1. Black Apple iPhone model# A1660 SIM# 8901260055977818269 07.00 PEAP# IS0001505865;
2. Gold Samsung Galaxy S7 IMEI# 3597750718140122 PEAP# IS0001505866;
3. Silver Apple iPhone model# A1688 PEAP# IS0001505867;
4. Black Apple iPhone SIM# 8901260073924670550M21.02 PEAP# IS0001505868;
5. Black Apple iPhone SIM# SM128PSIMT5TOD8901260955188263736 PEAP# IS0001505869;
6. Blue Samsung Galaxy S6 IMEI# 99000704798119316.07 PEAP# IS0001505870;
7. Gold Apple iPhone SIM# 89014104274488AO40262888773335 PEAP# IS0001505871;
8. Black Samsung Galaxy S7 PEAP# IS0001505872;
9. Blue Samsung Galaxy S6 IMEI# 9900070494339516.11 PEAP# IS0001505873;
10. Black Apple iPhone PEAP# IS0001505874;
11. Blue Apple iPhone SIM# 89148000006497258234 PEAP# IS0001505875;
12. Red Apple iPhone SIM# 8901260241733339903108648 PEAP# IS0001505876;
13. Black Samsung Galaxy S7 IMEI# 359764081434928 PEAP# IS0001505877;
14. Silver Samsung Galaxy S8 IMEI# 357723081373066 PEAP# IS0001505878;
15. Silver Samsung Galaxy S7 IMEI# 358166075659265 PEAP# IS0001505879;
16. Silver Apple iPhone model# A1586 IMEI# 359263067022856 PEAP# IS0001505880;

17. Gold Apple iPhone model# A1586 IMEI# 356977062704829 PEAP# IS0001505881.

Some of the **TARGET DEVICES** are locked or damaged preventing investigators from obtaining additional specific identifying phone information such as a model or serial number. The **TARGET DEVICES** are currently stored in the custody of the USPIS at 6500 Air Cargo Road, Oklahoma City, Oklahoma 73195 (Western District of Oklahoma).

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1708 (mail theft); 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); and 18 U.S.C. § 1349 (conspiracy to commit mail or wire fraud) (hereinafter the "TARGET OFFENSES") and involve Jason Fredy Darbouze, Nathan Tyrell Omega, Donald Preston Brown III, Evans Soiuilien, and Dimitris Shamar Simon, occurring after May 4, 2021, including:

a. Records, information, and communications, in any form, relating to, reflecting, and evidencing violations of the TARGET OFFENSES;

b. Any and all records, receipts, items, and documents reflecting the use of the interstate wire communications, including use of the Internet, in furtherance of the TARGET OFFENSES;

c. Books, records, receipts, notes, ledgers, notebooks, folders, ledgers, diaries, bank records, money orders, currency, wage statements, computer files, job applications, calendars, and correspondence, including correspondence to and from the Oklahoma Employment Security Commission (OESC) and any other unemployment insurance agency in any state of the United States, related to the filing of fraudulent unemployment insurance claims;

d. Debit cards, including, but not limited to debit cards issued by US Bank, or any other financial institution, or OESC, checks issued by the OESC or any other unemployment insurance agency in any state of the United

States; direct deposit forms for any financial institution, or any documentation relating to access devices believed to be used for the purpose of fraud;

e. Records, information, and communications, in any form, which relate to the identification of individuals who were victims of the TARGET OFFENSES;

f. Records, information, and communications, in any form, which relate to the identity or location (historic or current) of participants, co-conspirators, or aiders and abettors of the TARGET OFFENSES;

g. Records, information, and communications, in any form, which relate to the personal or business relationships between participants in the TARGET OFFENSES;

h. Communications, in any form, between the participants in the TARGET OFFENSES;

i. Records, information, and communications, in any form, which relate to the identity or location of criminally-derived property;

j. Records, information, and communications, in any form, concerning financial accounts and transactions related to the TARGET OFFENSES;

k. United States currency, cash counting machines, cryptocurrency, including but not limited to, bitcoin and stored on electronic and paper wallets or other means, cryptocurrency private keys and recovery seeds, gift cards, cash cards, and records relating to income derived from the

fraud scheme and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, checkbooks, check registers, securities, precious metals, jewelry, antique or modern automobiles, bank statements and other financial instruments, including stocks or bonds in amounts indicative of the proceeds of the fraud scheme;

l. Computers, storage media, or electronic devices used as a means to commit the violations described above, or that contain any of the items listed above;

m. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage;

2. Evidence of user attribution showing who used or owned the Target Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

MANNER OF SEARCH AS TO VIDEOS, PHOTOGRAPHS, AND STORED COMMUNICATIONS

1. Based upon my training and experience, I know that relevant and/or incriminating text or voice messages, videos, and photographs oftentimes are comingled on cellular telephones and electronic handheld devices with text messages, videos, and photographs which do not have an evidentiary value. However, criminals engaged in communications furthering the nature of their criminal enterprise often use cryptic, guarded, or otherwise coded jargon, which is often utilized to conceal the nature of their illegal communication. As a result, a limited review of the content of each communication will be necessary to determine the nature of the communication and whether it is relevant to that information particularly set forth above within this affidavit.

2. Searching the **TARGET DEVICES** for the evidence described above may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a keyword search that searches through the files stored in an electronic device for special words that are likely

to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directories or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the device's memory not allocated to listed files or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, I request permission to use whatever data analysis techniques necessary to locate and retrieve the evidence described above.